Settlement Agreement and Mutual Release - Security

EXHIBIT 2

ORCA Priority 1 Remediation Plan ("P-1")

ORCA Priority 1 Remediation Plan

Executive Summary

The Joint Board tasked the ORCA Technology Leadership Committee (TLC) to develop a comprehensive remediation plan, addressing critical technology risks as required to achieve a healthy system state. Given the magnitude of the effort, the TLC recommended a phased approach, focusing first on the highest priority issues. This document details the Priority 1 work plan, including the scope, schedule, and budget to remediate the highest priority system issues and risks.

The scope of the Priority 1 work plan is to resolve known critical system vulnerabilities and remediate the highest priority risk areas associated with PCI non-compliance and systems obsolescence. Findings to date indicate numerous system components are already out of compliance, and additional major components are pending non-compliance, notably Windows XP in April 2014. The recommended approach is to upgrade and remediate the unsupported, high risk systems components that directly store and process credit card data. The scope of work also requires each agency to isolate ORCA components on agency networks to secure the Cardholder Data Environment.

Addressing these short-term Priority 1 items will remediate major risks, closing the gap toward achieving a PCI Compliant ORCA system. Given that PCI necessitates strong operational processes in addition to secure system architecture, the TLC recognizes that there may be additional work to ultimately achieve compliance. This includes revisiting the regional approach to system auditing.

The Priority 1 work plan will require resources from Vix and from each Agency. Agency resources will be needed for testing, component isolation on agency networks, and commissioning upgraded system components. This will include technical staff familiar with agency networks, servers, and workstations, as well as business staff necessary for component testing.

The target completion for all Priority 1 components is 10 months from when the Joint Board authorizes work to begin. This date is aggressive, but manageable if each Agency and Vix agrees to complete this critical remediation work as the highest priority, and assigns the resources to complete the effort.

The total cost to complete the Priority 1 work plan is $1.97 million. This includes Vix development costs, Vix professional services costs, new computer hardware and licensing needed to replace obsolete systems, and third party PCI consulting services. This does not include any costs for each agency to complete requisite agency-level network architecture updates, nor does it include agency staff resources. This also does not include the cost of P2 and P3 remediation items, which will be presented at a future date.

The TLC will continue to provide guidance to Vix and the Agencies throughout remediation effort. The TLC will serve as the escalation point for issues, and will report remediation status to the Joint Board at their regularly scheduled meetings.

Version 2 Release Notes

This document is version 2.0 of the Priority 1 work plan. The original version 1.0 was issued on 12-2-2013. Updates from the previous version are highlighted blue within the body of the document below.

Scope of Work

The scope of the Priority 1 work plan is organized into seven major categories; each represents critical risk areas associated with PCI and End of Life / obsolescence. The remediation categories are:

1. Customer Service Terminal (CST) Upgrades
2. Back Office Computer (BOC) and BOC Client (BCC) Upgrades
3. Java Upgrades
4. JBoss Upgrades
5. Oracle Client Upgrades
6. Additional Back Office Upgrades
7. ORCA Network Security and Segmentation

1 – Customer Service Terminal (CST) Upgrades

All CSTs within the ORCA system currently run on the latest version of Windows XP Service Pack 3. Microsoft will stop releasing security patches for Windows XP when support ends in April 2014. As security exploits are identified for the Windows XP platform, risk to the ORCA environment will increase. In any case, continuing to run Windows XP on the CSTs will prohibit PCI compliance after April 2014.

The CST scope of work is to upgrade all CSTs and mobile CSTs to Windows 8, upgrade the MS Retail software to the latest supported Service Pack from Microsoft, and refresh all aged CST computer workstations. The MS Retail upgrade effort includes upgrading the Point of Sale databases on the BOCs to Microsoft SQL Server 2008. This is a technical upgrade effort, with no functional system enhancements outside what comes with the new Windows platform and software updates. This project requires a high level of effort from Vix software developers to update CST application functions to run in Windows 8. This development work represents the bulk of the CST upgrade cost and effort, and is the main constraint on the delivery timeline.

The remaining scope of work is to replace all aged CST computer workstations. Although not required for PCI compliance, the CSTs were purchased over five years ago and are beyond industry standard useful life. All fixed workstation CSTs will be replaced with new PC hardware and monitors. The intent is to keep the current ORCA specific CST peripherals to the extent possible. For the mobile CSTs (WPCSTs), the current hardware is relatively new, and does not require replacement at this time.

CST P1 Issues:

Device	Issue	End State	End of Life	PCI Req?
CST	Runs Windows XP SP3	Upgrade to Windows 8.1	Apr-14	Yes
CST	Runs MS Retail v2.0 SP2	Upgrade to current version		Yes

Device	Issue	End State	End of Life	PCI Req?
		(Includes BOC SQL 2008 upgrade)		
WPCST	Runs Windows XP SP3	Upgrade to Windows 8.1	Apr-14	Yes
WPCST	Runs MS Retail v2.0 SP2	Upgrade to current version (Includes BOC SQL 2008 upgrade)		Yes
CST	Hardware is obsolete	Replace with Dell Optiplex 3020s	Purchased 2008	No
BOC	SQL Server 2000	SQL Server 2008	Apr-13	Yes

Schedule:

1. Begin CST Development Effort 6-Jan-2014
2. Order CST Hardware 1-Aug-2014
3. Delivery to Regional Test Bed 29-Aug-2014
4. Vix Testing 1-Sep-2014
5. Agency Testing 29-Sep-2014
6. CSTs Deployed to Production 24-Oct-2014

Cost:

Vix Development	381,905
Vix Seattle Professional Services	31,115
CST Hardware (40 + 7 for Dev/Test)	74,503
CST Peripherals*	20,000
CST Software	8,229
Total	**$515,752**

***The intent is to keep the existing ORCA specific peripheral equipment to the extent possible. The allowance will only be used as needed to replace equipment that is not compatible with Windows 8.**

The cost for the CST upgrade is approximately $80,000 greater than what was identified in the earlier P1 plan. The original cost was based on a more current, but not the latest release of the MS Retail software. The latest release represents significant fundamental architecture changes that increase the need for development resources to adapt the ORCA system, thus the increase in cost. Although the latest release does not provide any additional functional capabilities, it is the current version supported by Microsoft and therefore maintains currency and reduces risks by eliminating unsupported software. The TLC has recommended that we move to this latest release now.

2 – BOC and BOC Client (BCC) Upgrades

The security risks to the BOCs are that they currently run unsupported versions of Oracle Database and Microsoft SQL Server (for the Point of Sale database) and as a result no longer receive security patches to vulnerabilities associated with those databases. Running these databases on unsupported versions puts the ORCA system at risk and prevents PCI compliance. The BOC scope of work is to upgrade all BOCs to Oracle 11 and SQL Server 2008 (included above as part of the CST upgrades) and refresh all

aged BOC server hardware which is beyond industry standard useful life. This is a technical upgrade effort, with no functional system enhancements. This project requires a high level of effort from Vix software developers to update BOC application functions to run with Oracle 11.

Due to the complexities of the BOC upgrade, the Perth Development Team performed a one month BOC upgrade analysis project as a prerequisite to providing a quote. As a result of this analysis, Vix has determined that the fixed price quote is $31,207 less than the ROM estimate previously provided. The fixed price quote for the development effort and revised schedule for delivery are reflected below.

In anticipation of future DAC upgrade work, the proposal is to virtualize the BOC on the physical replacement server. If the Agencies choose to later add an additional DAC server, virtualization across the two physical hosts can offer better redundancy than what is currently in place. Although hardware upgrades are not necessary to PCI, the current BOC servers are beyond industry standard useful life. The new server hardware will provide improved scalability and redundancy going forward.

The BOC Client scope of work includes upgrading the BCCs from Windows XP SP3 to Windows 8.1, and replacing outdated PC hardware. Also, the BCCs are included in the Network Segmentation effort (detailed in later section) to remove them from PCI scope altogether. The only development work required to accommodate the Windows 8.1 upgrade is the Java Upgrade (see the next section), so no costs apart from software licenses, new PCs, and professional services (for installation, etc) are included.

BOC/BCC P1 Issues:

Device	Issue	End State	End of Life	PCI Req?
BOC	Hardware is obsolete	Replace with PowerEdge R520 Server	Purchased 2008	No
BOC	Runs Oracle 10.2.0.4	Upgrade to Oracle 11.x	Jul-13	Yes
BCC	Runs Windows XP SP3	Upgrade to Windows 8	Apr-14	Yes
BCC	Hardware is obsolete	Replace with current Dell hardware	Purchased 2008	No

Schedule:

1. Begin BOC Upgrade Analysis 6-Jan-2014
2. Begin BOC Development 3-Mar-2014
3. Order BOC Hardware 1-Jun-2014
4. Delivery to Regional Test Bed 29-Aug-2014
5. Vix Testing 1-Sep-2014
6. Agency Testing 29-Sep-2014
7. BOC Deployed to Production 24-Oct-2014

Cost:

Vix Development - BOC Upgrade Analysis	14,172
Vix Development - BOC Upgrade	93,793

Vix Seattle Professional Services	31,115
BOC Hardware (7 + 2 for Dev/Test)	107,010
BOC Software (Windows Server and vSphere licenses)	29,967
BCC Replacements (Windows 8 PCs)	11,942
Total	**$287,999**

3 – Java Upgrades

ORCA systems currently run an outdated version of Java (6.0.21), which is no longer supported as of Feb-2013. This was a PCI finding in the 2013 PCI Audit, and represents an ongoing security risk to the system. This risk is currently mitigated by good perimeter security and restricted logical access to these systems (via the firewall and 24x7 intrusion detection).

The Java Upgrades scope of work is to upgrade all systems running Java 6 to run the current version. This is a technical upgrade effort, with no functional system enhancements. This project requires a medium level of effort from Vix software developers to update ORCA application functions to run with Java 7.x.

Java P1 Issues (This is not an exhaustive list of every system that runs Java. All ORCA systems that run Java will be upgraded to the current version as part of this effort):

Device	Issue	End State	End of Life	PCI Req?
CST	Runs Java 6.0.21	Upgrade to Java 7.x	Feb-13	Yes
WPCST	Runs Java 6.0.21	Upgrade to Java 7.x	Feb-13	Yes
BOC	Runs Java 6.0.21	Upgrade to Java 7.x	Feb-13	Yes
IWS	Runs Java 6.0.21	Upgrade to Java 7.x	Feb-13	Yes
MWS	Runs Java 6.0.21	Upgrade to Java 7.x	Feb-13	Yes
WEB	Runs Java 6.0.21	Upgrade to Java 7.x	Feb-13	Yes

Schedule:

1.	Begin Java Development	6-Jan-2014
2.	Delivery to Regional Test Bed	16-May-2014
3.	Vix Testing	19-May-2014
4.	Agency Testing	2-Jun-2014
5.	Java Deployed to Production	13-Jun-2014 (MR26)

Cost:

Vix Development	49,600
Vix Seattle Professional Services	16,878
Hardware	N/A
Software	N/A
Total	**$66,478**

4 – JBoss Upgrades

ORCA systems currently run an outdated version of JBoss (4.0.1) which is no longer supported by release of regular security patches as of Jun-2010. This was a PCI finding in the 2013 PCI Audit, and represents an ongoing security risk to the system. JBoss is the foundation for the ORCA web servers, and there are existing vulnerabilities to external-facing systems such as the public websites. JBoss vulnerabilities are a common target for hackers, and it is considered a critical system to keep secure. The risk of exploitation of these vulnerabilities is currently mitigated by good perimeter security and restricted logical access to these systems (via the firewall and 24x7 intrusion detection). Attacks targeting the ORCA websites are automatically detected and the offending IP addresses are blocked.

The JBoss Upgrades scope of work is to upgrade all systems running JBoss 4.0.1 to JBoss 7.1. This is a technical upgrade effort, with no functional system enhancements. This project requires a high level of effort from Vix software developers to update ORCA application functions to run with JBoss 7.1.

JBoss P1 Issues:

Device	Issue	End State	End of Life	PCI Req?
CST	Runs JBoss 4.0.1	Upgrade to JBoss 7.1	Jun-2010	Yes
WPCST	Runs JBoss 4.0.1	Upgrade to JBoss 7.1	Jun-2010	Yes
BOC	Runs JBoss 4.0.1	Upgrade to JBoss 7.1	Jun-2010	Yes
IWS	Runs JBoss 4.0.1	Upgrade to JBoss 7.1	Jun-2010	Yes
MWS	Runs JBoss 4.0.1	Upgrade to JBoss 7.1	Jun-2010	Yes
WEB	Runs JBoss 4.0.1	Upgrade to JBoss 7.1	Jun-2010	Yes
ACS	Runs JBoss 4.0.1	Upgrade to JBoss 7.1	Jun-2010	Yes

Schedule:

1.	Begin JBoss Development Effort	6-Jan-2014
2.	Delivery to Regional Test Bed	29-Aug-2014
3.	Vix Testing	1-Sep-2014
4.	Agency Testing	29-Sep-2014
5.	JBoss Deployed to Production	24-Oct-2014

Cost:

Vix Development	436,757
Vix Seattle Professional Services	31,115
Hardware	N/A
Software	N/A
Total	**$467,872**

5 – Oracle Client Upgrades

A number of ORCA systems that need to connect to the OFS Oracle Database do so via an outdated version of the Oracle Client (version 10.2.0.1). This version is no longer supported by Oracle with regular security patches for critical vulnerabilities. Any system running this version that is in scope for a PCI audit would be deemed non-compliant. The specific risk associated with running an older version of the Oracle client is low to medium: the Oracle database does store credit card information, but the associated risk is mitigated by using strong encryption to protect that stored credit card data and by restricting access to the database to back office systems. A perimeter (firewall) breach would be required to exploit any vulnerabilities associated with the Oracle Client software.

The Oracle Client Upgrades scope of work is to upgrade all systems running Oracle Client 10.x to Oracle Client 11.x. This is a technical upgrade effort, with no functional system enhancements. This project requires a high level of effort from Vix software developers to update ORCA application functions to run with Oracle Client 11. The Perth Development Team performed a one month Oracle Client Upgrade analysis project as a prerequisite to providing a quote. As a result of this analysis, Vix has determined that the fixed price quote is $25,014 less than the ROM estimate previously provided. The fixed price quote for the development effort and revised schedule for delivery are reflected below.

Oracle Client P1 Issues:

Device	Issue	End State	End of Life	PCI Req?
ACS	Oracle Client 10.2.0.1	Oracle 11.x	Jul-13	Yes
BCC	Oracle Client 10.2.0.1	Oracle 11.x	Jul-13	Yes
CDA	Oracle Client 10.2.0.1	Oracle 11.x	Jul-13	Yes
CDG	Oracle Client 10.2.0.1	Oracle 11.x	Jul-13	Yes
CST	Oracle Client 10.2.0.1	Oracle 11.x	Jul-13	Yes
WPCST	Oracle Client 10.2.0.1	Oracle 11.x	Jul-13	Yes
MWS	Oracle Client 10.2.0.1	Oracle 11.x	Jul-13	Yes
OLS	Oracle Client 10.2.0.1	Oracle 11.x	Jul-13	Yes

Schedule:

1. Begin Oracle Client Upgrade Analysis 6-Jan-2014
2. Begin Oracle Client Development 3-Mar-2014
3. Delivery to Regional Test Bed 29-Aug-2014
4. Vix Testing 1-Sep-2014
5. Agency Testing 29-Sep-2014
6. Oracle Client Deployed to Production 24-Oct-2014

Cost:

Vix Development - Oracle Client Upgrade Analysis 33,759

Vix Development - Oracle Client Upgrade	158,316
Vix Seattle Professional Services	16,878
Hardware	N/A
Software	N/A
Total	**$208,953**

6 – Additional Back Office Upgrades

There are three additional priority 1 work items in the Back Office which need to be addressed, based on the Vix 2013 PCI Audit. These items are:

1. Change Vix software distribution scripts to use SSH instead of FTP (which is insecure)
2. Upgrade the back office Online Server (OLS) from Solaris 9 to Solaris 10
3. Remediate the website vulnerabilities identified as part of the 2012 Penetration Testing performed against the back office.

The first two items will largely be handled by the Vix Seattle team as part of MR25 (or the closest release) since they require minimal development effort. The last item will be performed by Perth Development and delivered along with the Java upgrades.

Back Office P1 Issues:

Device	Issue	End State	End of Life	PCI Req?
ASA5550	FTP in use	Upgrade to use SSH	N/A	Yes
OLS	Runs Solaris 9	Upgrade to Solaris 10	Oct-2011	Yes
WEB	Penetration Test Findings	Remediate findings	N/A	Yes

Schedule:

1.	Begin Development	6-Jan-2014
2.	Delivery to Regional Test Bed	16-May-2014
3.	Vix Testing	19-May-2014
4.	Agency Testing	2-Jun-2014
5.	Deployed to Production	13-Jun-2014 (MR26)

Cost:

Vix Development	54,424
Vix Seattle Professional Services	33,757
Hardware	N/A
Software	N/A
Total	**$88,181**

7 - ORCA Network Security and Segmentation

The ORCA system currently contains several network-related components not in compliance with PCI-DSS requirements. Many of these issues are the responsibility of the agencies to resolve, as Vix does not have access to agency network resources. Both the Vix 2013 PCI Audit and the recent system architecture review by the ORCA TLC have identified network-related compliance issues. These include, but are not limited to, network security and segmentation of ORCA devices on agency networks such as CSTs, WAPs, BOCs, BCCs, DACs, and PFTPs. The networks on which these ORCA devices reside are part of the overall ORCA system, and require remediation to achieve PCI-DSS compliance.

The initial priority is remediating the ORCA system components with direct impact to the Cardholder Data Environment. Network segmentation includes clearly defining "in-scope" and "out-of-scope" ORCA components, updating network architecture, and limiting the scope of the Cardholder Data Environment. Achieving compliance will require a holistic, system-wide approach to network architecture as well as processes such as routine updates, patches and vulnerability scanning of ORCA components within the participating agencies.

In addition, the region will need to develop a new, common approach to PCI compliance since the current approach has not resulted in compliance to date. To complete this effort, the region will form an ORCA Network Remediation Team, under the guidance of the ORCA TLC. The team will consist of network security subject matter experts from each agency, and from Vix. The team will hire a third party Qualified Security Assessor (QSA) / PCI expert as a consultant to:

- Identify and advise on current risks/gaps
- Develop a common approach based on industry best practice
- Advise on the approach and efforts needed to reach full PCI compliance
- Advise and provide guidance on PCI specific questions

The Network Remediation Team will be responsible for re-engineering network architecture and processes as needed to meet PCI-DSS compliance standards, under the new approach. This includes providing an implementation plan for each Agency to achieve compliance. The team will also support each agency for guidance during implementation.

Network security information will be discussed to reach the common goal of getting the ORCA network, regionally, in PCI compliance. It is imperative that each Network Remediation Team member participate in an open, collaborative manner regarding their Agency's network configuration while also maintaining confidentiality of the Agencies' and Vix networks.

ORCA Network Security and Segmentation P1 Issues

Device	Issue	End State	End of Life	PCI Req?
CST	No penetration test	Perform annual penetration testing and remediate findings	N/A	Yes
CST	No vulnerability scans	Perform quarterly scans and	N/A	Yes

Device	Issue	End State	End of Life	PCI Req?
		remediate findings		
WDOL	WDOLs in scope for PCI	Network Segmentation to Limit PCI Scope	N/A	Yes
DAC	No penetration test	Network Segmentation to Limit PCI Scope	N/A	Yes
DAC	No vulnerability scans	Network Segmentation to Limit PCI Scope	N/A	Yes
DAC	DACs in scope for PCI	Network Segmentation to Limit PCI Scope	N/A	Yes
WAP	WAPs in scope for PCI	Network Segmentation to Limit PCI Scope	N/A	Yes
BOC	No penetration test	Perform annual penetration testing and remediate findings	N/A	Yes
BOC	No vulnerability scans	Perform quarterly scans and remediate findings	N/A	Yes
BCC	BCCs in scope for PCI	Network Segmentation to Limit PCI Scope	N/A	Yes
WDOL	WEP Security	Network Segmentation to Limit PCI Scope	N/A	Yes
WAP	WEP Security	Network Segmentation to Limit PCI Scope	N/A	Yes
Network	No Agency/Vix network boundary definitions	Define boundary of agency and Vix responsibilities	N/A	Yes

Schedule:

1. Form ORCA Network Remediation Team — Dec-2013
2. Define current network state; identify gaps — Jan-2014
3. Define future state; revised PCI approach, architecture — Feb-2014
4. Establish implementation schedule — Mar-2014
5. Implement new solution throughout all agencies — Sep-2014

Each Agency and Vix will assign a network security engineer to participate in the Network Remediation Team, to reach PCI-DSS compliance as a priority.

Cost:

3rd Party QSA Professional Services	$ 90,000
Vix Professional Services (for initial 4 months)*	$ 9,925
Agency Specific Costs**	Borne by each agency

*If new technical requirements are identified as part of the revised approach to PCI; any additional Vix Development costs and Vix Professional Services costs will be determined during the first four months, and included in a future work plan.

**Agency specific costs are directly dependent on the amount of ORCA equipment that each agency uses, the current network design, and the gaps identified for each agency to reach PCI compliance. Areas that may involve costs at each agency include, but are not limited to:

- Firewalls – Used to segment from other networks to allow secure communication with Vix and segment CDE (Cardholder Data Environment)
- Network switches – Provide physical network connectivity and security
- Network routers – Segment and route network traffic securely between appropriate networks.
- Wireless technologies – May need to implement technologies to secure wireless communications if not in place already.
- Professional Services – May be needed by agencies requiring additional technical support beyond staff resources

Budget

Total Combined Cost for P1 Work Plan:

Category	Cost
Customer Service Terminal Upgrade	515,752
Back Office Computer and Client Upgrades	287,999
Java Upgrades	66,478
JBoss Upgrades	467,872
Oracle Client Upgrades	208,953
Additional Back Office Upgrades	88,181
ORCA Network Security and Segmentation	99,925
Subtotal	1,735,160
Project Contingency	256,767
Net Increase for v2.0	23,383
Revised Contingency	233,384
Total	**$1,968,544**

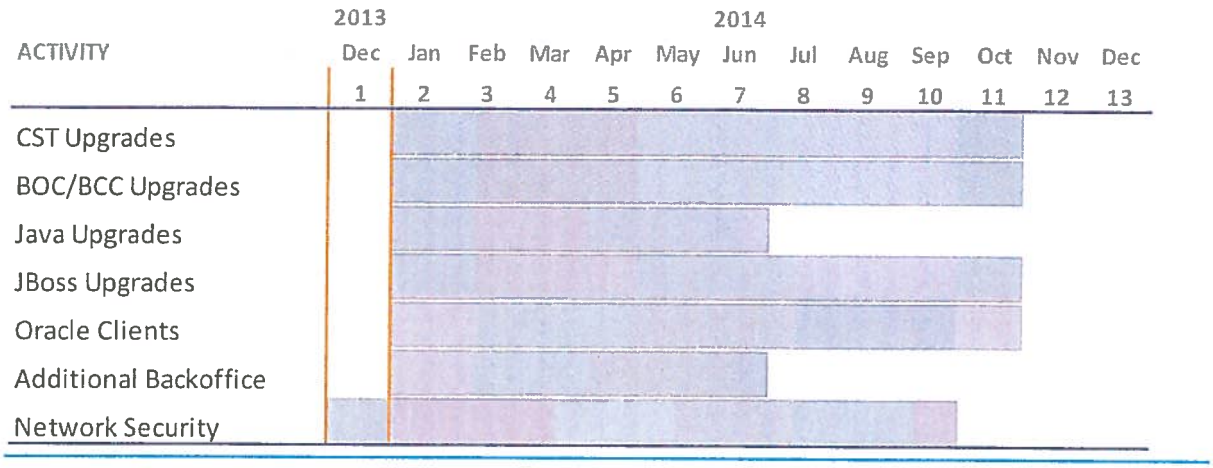
This is a good faith estimate to deliver the scope of work detailed in this work plan. Given the fast turnaround time to develop the work plan, there will likely be variances at the category level, but the bottom line total is considered a not to exceed amount to deliver the P1 work plan. Given the variables, a bottom line contingency has been added, but will require approval to utilize.

The above costs do not include any costs for each agency to complete requisite agency-level network architecture updates, nor does it include agency staff resources. This also does not include the cost of P2 and P3 remediation items, which will be presented at a future date.

Schedule

The delivery schedule for each category is summarized below.

ORCA P1 Work Plan



Recommended Payment Approach

The ORCA TLC recommends a milestone based payment approach for each of the seven project categories, including a 20% holdback to be paid upon final Production deployment. The payment milestones are not detailed in this work plan, and should be included in the contractual agreement that will allow this work plan to proceed.